

1 CLAIMS

2 What is claimed is:

3 1. A system comprising:

4 a plurality of certificate authorities (CAs) in which each CA  
5 maintains and distributes digital certificates revoked by itself in  
6 the form of a certificate revocation list (CRL), and different CAs  
7 may use different CRL distribution mechanisms;

8 a plurality of CRL databases for storing the consolidated CRLs from  
9 multiple CRL retrieval agents and/or the replications of CRLs; and

10 a CRL access user interface for providing a uniform set of APIs for  
11 user's accessing the CRLs CRL databases, said system enabling  
12 consolidation and access of the certificate revocation list (CRL).

13 2. A system according to claim 1, wherein said plurality of CRL  
14 databases include a central CRL database and a plurality of CRL  
15 replication databases, said central CRL database for storing the  
16 consolidated CRLs from the multiple CRL retrieval agents, and said  
17 plurality of CRL replication databases for storing the replications  
18 of the CRLs of the central CRL database.

19 3. A system according to claim 1, wherein said plurality of CRL  
20 retrieval agents include a LDAP/CRL retrieval agent, for  
21 periodically retrieving CRLs from specified LDAP servers and  
22 updating the CRL databases.

1 4. A system according to claim 1, wherein said plurality of CRL  
2 retrieval agents include a HTTP/CRL retrieval agent, for  
3 periodically retrieving CRLs from specified HTTP servers and  
4 updating the CRL database.

5 5. A system according to claim 1, wherein said plurality of CRL  
6 retrieval agents include a RFC1424/CRL retrieval agents, for  
7 periodically sending RFC1424/CRL retrieval request and receiving  
8 CRL retrieval reply.

9 6. A system according to claim 1, wherein said plurality of CRL  
10 retrieval agents include a Http receiver agent triggered by a HTTP  
11 request, said Http receiver agent verifies an authorization of the  
12 requester, if successful, said agent stores each transmitted CRL in  
13 the CRL databases.

14 7. A system according to claim 1, wherein said plurality of CRL  
15 retrieval agents further verifies the integrity and the  
16 authenticity of the retrieved CRLs.

17 8. A system according to claim 1, wherein a particular replication  
18 architecture is used among said plurality of CRL databases in order  
19 to maintain database consistency.

20 9. A system according to claim 2, wherein a sub-and-spoke  
21 replication architecture is used among said central CRL database  
22 and said plurality of CRL replication databases.

23 10. A system according to claim 1, wherein said system is also  
24 adapted for consolidating and accessing at least one kind of black  
25 list.

1 11. In a secure network implemented by digital certificates, a  
2 method for certificate revocation list (CRL) consolidation and  
3 access, wherein a plurality of certificate authorities (CAs)  
4 maintain and distribute the digital certificates revoked by  
5 themselves in the form of CRLs, and different CAs may use different  
6 CRL distribution mechanisms, said method comprising the steps of:

7 creating a plurality of CRL retrieval agents based on the CRL  
8 distribution mechanisms of CAs, for consolidating the CRLs from  
9 multiple CAs;

10 storing the consolidated CRLs from multiple CRL retrieval agents or  
11 the replications of CRLs into a plurality of CRL databases; and

12 accessing the CRLs from the CRL databases by a uniform set of APIs.

13 12. A method according to claim 11, said plurality of CRL databases  
14 include a central CRL database and a plurality of CRL replication  
15 database, said central CRL database for storing the consolidated  
16 CRLs from multiple CRL retrieval agents and said plurality of CRL  
17 replication database for storing the replications of the CRLs of  
18 the central database.

19 13. A method according to claim 11, wherein said method is also  
20 adapted for consolidating and accessing all kinds of black lists.

21 14. An article of manufacture comprising a computer usable medium  
22 having computer readable program code means embodied therein for  
23 causing certificate revocation list (CRL) consolidation and  
24 access,, the computer readable program code means in said article

1 of manufacture comprising computer readable program code means for  
2 causing a computer to effect the steps of claim 11.

3 15. A computer program product comprising a computer usable medium  
4 having computer readable program code means embodied therein for  
5 causing certificate revocation list (CRL) consolidation and access,  
6 the computer readable program code means in said computer program  
7 product comprising computer readable program code means for causing  
8 a computer to effect the steps of claim 11.

9 17. A program storage device readable by machine, tangibly  
10 embodying a program of instructions executable by the machine to  
11 perform method steps for certificate revocation list (CRL)  
12 consolidation and access, said method steps comprising the steps of  
13 claim 11.

14 18. A method comprising:

15 employing a secure network implemented by digital certificates for  
16 certificate revocation list (CRL) consolidation and access, with a  
17 plurality of certificate authorities (CAs) maintaining and  
18 distributing the digital certificates revoked by themselves in the  
19 form of CRLs, wherein different CAs may use different CRL  
20 distribution mechanisms, including the steps of:

21 creating a plurality of CRL retrieval agents based on the CRL  
22 distribution mechanisms of CAs, for consolidating the CRLs from  
23 multiple CAs;

24 storing the consolidated CRLs from multiple CRL retrieval agents or  
25 the replications of CRLs into a plurality of CRL databases; and

1   accessing the CRLs from the CRL databases by a uniform set of APIs.

2   19. A program storage device readable by machine, tangibly  
3   embodying a program of instructions executable by the machine to  
4   perform method steps for certificate revocation list (CRL)  
5   consolidation and access, said method steps comprising the steps of  
6   claim 18.

7   20. An article of manufacture comprising a computer usable medium  
8   having computer readable program code means embodied therein for  
9   causing certificate revocation list (CRL) consolidation and access,  
10   the computer readable program code means in said article of  
11   manufacture comprising computer readable program code means for  
12   causing a computer to effect the steps of claim 18.

13   21. A computer program product comprising a computer usable medium  
14   having computer readable program code means embodied therein for  
15   causing certificate revocation list (CRL) consolidation and access,  
16   the computer readable program code means in said computer program  
17   product comprising computer readable program code means for causing  
18   a computer to effect the steps of claim 18.